Network Working Group
Internet Draft
draft-ietf-ipsec-sctp-05.txt

S. M. Bellovin
J. Ioannidis
AT&T Labs - Research
A. D. Keromytis
Columbia University
R. R. Stewart
Cisco

On the Use of SCTP with IPsec

Status of this Memo

Abstract

This document describes functional requirements for IPsec [RFC2401] and IKE [RFC2409] to facilitate their use in securing SCTP [RFC2960] traffic.

1. Introduction

The Stream Control Transmission Protocol (SCTP) is a reliable transport protocol operating on top of a connection-less packet network such as IP. SCTP is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications.

When SCTP is used over IP networks, it may utilize the IP security protocol suite [RFC2402][RFC2406] for integrity and confidentiality. To dynamically establish IPsec Security Associations (SAs), a key negotiation protocol such as IKE [RFC2409] may be used.

This document describes functional requirements for IPsec and IKE to facilitate their use in securing SCTP traffic. In particular, we discuss additional support in the form of a new ID type in IKE [RFC2409] and implementation choices in the IPsec processing to

accommodate for the multiplicity of source and destination addresses associated with a single SCTP association.

1.1. Terminology

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC-2119].

2. SCTP over IPsec

When utilizing the Authentication Header [RFC2402] or Encapsulating Security Payload [RFC2406] protocols to provide security services for SCTP frames, the SCTP frame is treated as just another transport layer protocol on top of IP (same as TCP, UDP, etc.)

IPsec implementations should already be able to use the SCTP transport protocol number as assigned by IANA as a selector in their Security Policy Database (SPD). It should be straightforward extend existing implementations to use the SCTP source and destination port numbers as selectors in the SPD. Since the concept of a port, and its location in the transport header is protocol-specific, the IPsec code responsible for identifying the transport protocol ports has to be suitable modified. This, however is not enough to fully support the use of SCTP in conjunction with IPsec.

Since SCTP can negotiate sets of source and destination addresses (not necessarily in the same subnet or address range) that may be used in the context of a single association, the SPD should be able to accommodate this. The straightforward, and expensive, way is to create one SPD entry for each pair of source/destination addresses negotiated. A better approach is to associate sets of addresses with the source and destination selectors in each SPD entry (in the case of non-SCTP traffic, these sets would contain only one element). While this is an implementation decision, implementors are encouraged to follow this or a similar approach when designing or modifying the SPD to accommodate SCTP-specific selectors.

Similarly, SAs may have multiple associated source and destination addresses. Thus an SA is identified by the extended triplet ({set of destination addresses}, SPI, Security Protocol). A lookup in the Security Association Database (SADB) using the triplet (Destination Address, SPI, Security Protocol), where Destination Address is any of the negotiated peer addresses, MUST return the same SA.

When operating in tunnel mode, the question of what to use as the tunnel destination address (for the `outer' header) arises. We distinguish three cases: where the end hosts are also the tunnel

endpoints; where neither host is a tunnel endpoint (the tunnel endpoints are security gateways); and where only one of the hosts is a tunnel endpoint (the usual case for the `road warrior' talking to a security gateway). In the first case, the outer addresses MUST be the same as the inner addresses of the tunnel. In the second case (security gateways) there is no special processing; address selection proceeds as it would for two distinct sets of end hosts. In the third case, the `road warrior' uses the security gateway's address as the tunnel destination address, and MUST use the same source address as that of the inner packet. Symmetrically, the security gateway uses its own address as the source address of the tunnel, and MUST use the the same destination address in the outer header as that of the inner packet. An implementation will probably structure the code so that if, during SA setup, the inner and outer address of either side is the same, rather than explicitly store the corresponding address of the tunnel, it sets a flag that marks the SA to use the same address in the tunnel header as in the inner header.

3. SCTP and IKE

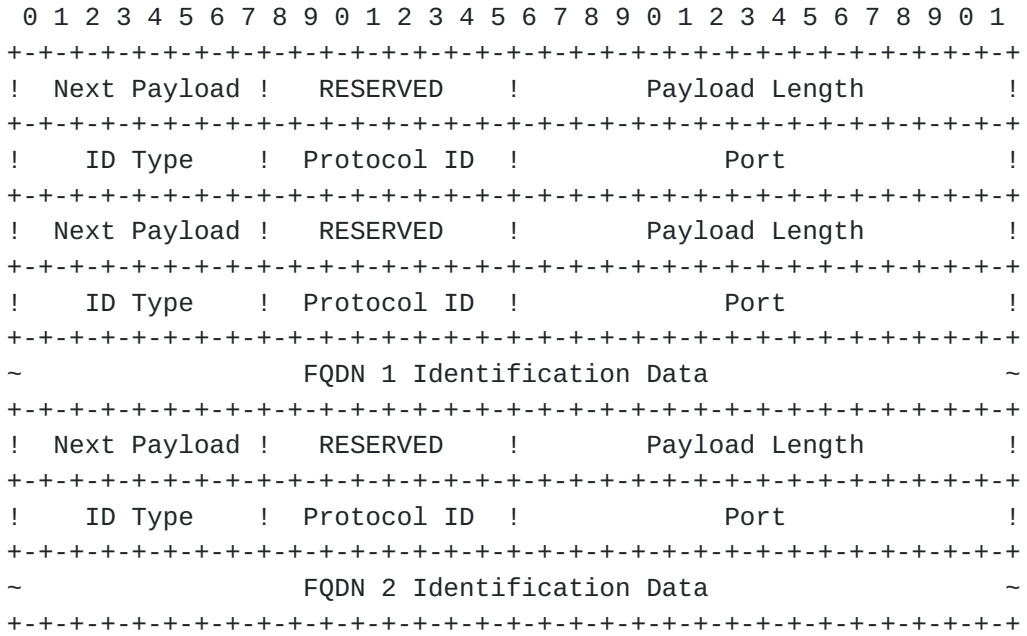
There are two issues relevant to the use of IKE when negotiating protection for SCTP traffic:

a) Since SCTP allows for multiple source and destination network addresses associated with an SCTP association, it MUST be possible for IKE to efficiently negotiate these in the Phase 2 (Quick Mode) exchange. The straightforward approach is to negotiate one pair of IPsec SAs for each combination of source and destination addresses. This can result in an unnecessarily large number of SAs, thus wasting time (in negotiating these) and memory. All current implementations of IKE support this functionality. However, a method for specifying multiple selectors in Phase 2 is desirable for efficiency purposes. Compliance with this document requires that implementations adhere to the guidelines in the rest of this section.

Define a new type of ID, ID_LIST, that allows for recursive inclusion of IDs. Thus, the IKE Phase 2 Initiator ID for an SCTP association MAY be of type ID_LIST, which would in turn contain as many ID_IPV4_ADDR IDs as necessary to describe Initiator addresses; likewise for Responder IDs. Note that other selector types MAY be used when establishing SAs for use with SCTP, if there is no need to use negotiate multiple addresses for each SCTP endpoint (i.e., if only one address is used by each peer of an SCTP flow). Implementations MUST support this new ID type.

ID_LIST IDs cannot appear inside ID_LIST ID payloads. Any of the ID types defined in [RFC2407] can be included inside an ID_LIST ID. Each of the IDs contained in the ID_LIST ID must include a complete Identification Payload header.

The following diagram illustrates the content of an ID_LIST ID payload that contains two ID_FQDN payloads.



The Next Payload field in any of the included IDs (for FQDN 1 and FQDN 2) MUST be ignored by the Responder. The Payload Length, ID Type, Protocol ID, and Port fields of the included Payloads should be set to the appropriate values. The Protocol ID and Port fields of the ID_LIST Payload should be set to zero by the Initiator and ignored by the Responder.

Different types of IDs (e.g., an ID_FQDN and an ID_IPV4_ADDR) can be included inside the same ID_LIST ID. If an ID type included in an ID_LIST ID payload is invalid in the context the ID_LIST ID is used, the whole ID_LIST should be considered to be at fault, e.g., if an ID_LIST ID payload that contains an ID_FQDN and an ID_IPV4_ADDR is received during an IKE Quick Mode exchange, the Responder should signal a fault to the Initiator and stop processing of the message (the same behavior it would exhibit if simply an ID_FQDN was received instead).

The IANA-assigned number for the ID_LIST ID is [TBD].

b) For IKE to be able to validate the Phase 2 selectors, it must be possible to exchange sufficient information during Phase 1. Currently, IKE can directly accommodate the simple case of two machines talking to each other, by using Phase 1 IDs corresponding to their IP addresses, and encoding those same addresses in the SubjAltName of the certificates used to authenticate the Phase 1 exchange. For more complicated scenarios, external policy (or some

other mechanism) needs to be consulted, to validate the Phase 2 selectors and SA parameters. All addresses presented in Phase 2 selectors MUST be validated. That is, enough evidence must be presented to the Responder that the Initiator is authorized to receive traffic for all addresses that appear in the Phase 2 selectors. This evidence can be derived from the certificates exchanged during Phase 1 (if possible); otherwise it must be acquired through out-of-band means (e.g., policy mechanism, configured by the administrator, etc.).

In order to accommodate the same simple scenario in the context of multiple source/destination addresses in an SCTP association, it MUST be possible to:

1) Specify multiple Phase 1 IDs, which are used to validate Phase 2 parameters (in particular, the Phase 2 selectors). Following the discussion on an ID_LIST ID type, it is possible to use the same method for specifying multiple Phase 1 IDs.

2) Authenticate the various Phase 1 IDs. Using pre-shared key authentication, this is possible by associating the same shared key with all acceptable peer Phase 1 IDs. In the case of certificates, we have two alternatives:

   a) The same certificate can contain multiple IDs encoded in the SubjAltName field, as an ASN.1 sequence. Since this is already possible, it is the preferred solution and any compliant implementations MUST support this.

   b) Multiple certificates MAY be passed during the Phase 1 exchange, in multiple CERT payloads. This feature is also supported by the current specification. Since only one signature may be issued per IKE Phase 1 exchange, it is necessary for all certificates to contain the same key as their Subject. However, this approach does not offer any significant advantage over (a), thus implementations MAY support it.

   In either case, an IKE implementation needs to verify the validity of a peer's claimed Phase 1 ID, for all such IDs received over an exchange.

Although SCTP does not currently support modification of the addresses associated with an SCTP association (while the latter is in use), it is a feature that may be supported in the future. Unless the set of addresses changes extremely often, it is sufficient to do a full Phase 1 and Phase 2 exchange to establish the appropriate selectors and SAs.

The last issue with respect to SCTP and IKE pertains to the initial

offer of Phase 2 selectors (IDs) by the Initiator. Per the current IKE specification, the Responder must send in the second message of the Quick Mode the IDs received in the first message. Thus, it is assumed that the Initiator already knows all the Selectors relevant to this SCTP association. In most cases however, the Responder has more accurate knowledge of its various addresses. Thus, the IPsec Selectors established can be potentially insufficient or inaccurate.

If the proposed set of Selectors is not accurate from the Responder's point of view, the latter can start a new Quick Mode exchange. In this new Quick Mode exchange, the roles of Initiator and Responder have been reversed; the new Initiator MUST copy the SA and Selectors from the old Quick Mode message, and modify its set of Selectors to match reality. All SCTP-supporting IKE implementations MUST be able to do this.

4. Security Considerations

This documents discusses the use of a security protocol (IPsec) in the context of a new transport protocol (SCTP). SCTP, with its provision for mobility, opens up the possibility for traffic-redirection attacks whereby an attacker X claims that his address should be added to an SCTP session between peers A and B, and be used for further communications. In this manner, traffic between A and B can be seen by X. If X is not in the communication path between A and B, SCTP offers him new attack capabilities. Thus, all such address updates of SCTP sessions should be authenticated. Since IKE negotiates IPsec SAs for use by these sessions, IKE MUST validate all addresses attached to an SCTP endpoint either through validating the certificates presented to it during the Phase 1 exchange, or through some out-of-band method.

The Responder in a Phase 2 exchange MUST verify the Initiator's authority to receive traffic for all addresses that appear in the Initiator's Phase 2 selectors. Not doing so would allow for any valid peer of the Responder (i.e., anyone who can successfully establish a Phase 1 SA with the Responder) to see any other valid peer's traffic by claiming their address.

5. IANA Considerations

IANA must assign a number for ID_LIST (defined in Section 3) in the "IPSEC Identification Type" registry from the Internet Security Association and Key Management Protocol (ISAKMP) Identifiers table.

References:

[Bel96] Steven M. Bellovin, "Problem Areas for the IP Security

Protocols", Proceedings of the Sixth Usenix Unix Security Symposium, July, 1996.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMPD", RFC 2407, November 1998.

[RFC2408] Maughan, D., Schertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol", RFC 2408, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

Authors' addresses:

Steven M. Bellovin
AT&T Labs - Research
180 Park Avenue
Florham Park, New Jersey 07932-0971

Email: smb@research.att.com

John Ioannidis
AT&T Labs - Research
180 Park Avenue
Florham Park, New Jersey 07932-0971

Email: ji@research.att.com

Angelos D. Keromytis
Columbia University, CS Department
515 CS Building
1214 Amsterdam Avenue, Mailstop 0401
New York, New York 10027-7003

Phone: +1 212 939 7095
Email: angelos@cs.columbia.edu

Randall R. Stewart
24 Burning Bush Trail.
Crystal Lake, IL 60012

Phone: +1-815-477-2127
Email: rrs@cisco.com

Expiration and File Name

This draft expires in October 2003

Its file name is draft-ietf-ipsec-sctp-05.txt